UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA	)	
	)	
v.	)	Case No. 5:12-cr-37
	)	
DEREK THOMAS	)	

OPINION AND ORDER DENYING
DEFENDANT'S MOTION TO SUPPRESS
(Doc. 28)

This matter came before the court on September 20, 2012 for an evidentiary hearing on Defendant Derek Thomas's motion to suppress. (Doc. 28.) Defendant is charged with knowing possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B).

Defendant seeks suppression of all evidence seized during a search of his residence on March 2, 2012, arguing that the search warrant was invalid because of material omissions from the supporting affidavit (the "Affidavit"). The Government opposes the motion.

Defendant is represented by Federal Public Defender Michael L. Desautels. The Government is represented by Assistant U.S. Attorney Nancy J. Creswell.

I. Findings of Fact.

On approximately December 21, 2011, officers with the South Burlington Police Department discovered an Internet Protocol ("IP") address that had previously offered to share files containing child pornography on the Internet through peer-to-peer file sharing (the "IP Address"). The IP Address was assigned to Comcast. A Special Agent with Homeland Security Investigations ("HSI") served a subpoena on Comcast requesting identification of the subscriber to the IP Address. Comcast responded that the IP Address

was registered to Diane Jarvis, who lived at 73 Granite Creek Road, Colchester, Vermont, 05446 (the "Residence").[1]

Upon receiving this information, HSI Special Agent Seth Fiore verified that Ms. Jarvis lived at the Residence by running checks with a service identified as "Clear" and with the Vermont State Police's database. Agent Fiore also engaged in surveillance of the Residence on several different dates. During his surveillance, Agent Fiore ran the license plate of a vehicle at the Residence, and found that it was registered to Ms. Jarvis. According to Agent Fiore, the purpose of his surveillance was to confirm that Ms. Jarvis lived at the Residence, to verify for officer safety whether any other individuals lived there, and to ascertain whether there were children living at the Residence.

During the surveillance, Agent Fiore used two different electronic devices for identifying wireless networks (each a "Portable Wireless Detector"). The Portable Wireless Detectors purport to identify wireless networks in a particular area and indicate whether the wireless networks are password protected. Although Agent Fiore had not received formal training in the use of the Portable Wireless Detectors, HSI Special Agent McCullough, who works in computer forensics, advised Agent Fiore regarding their proper use and how to decode the information they displayed.

On February 1, 2012, Agent Fiore used one of the Portable Wireless Detectors in the street outside of the condominium complex in which the Residence is located. During this reading, the Portable Wireless Detector identified fifteen active wireless networks. Five of the networks were unsecure. None of the wireless networks identified on February 1 were clearly connected with the Residence. On February 7, 2012, Agent Fiore utilized the second Portable Wireless Detector in the driveway of the Residence. The second Portable Wireless Detector identified seven wireless networks, one of which was unsecure. During this second surveillance, Agent Fiore observed a wireless network

[1] An IP address is not necessarily associated with a single computer. Rather, a wireless router can be used to allow multiple computers to access the Internet using the same IP address. Therefore, it is possible that a person could utilize an IP address associated with an unsecure wireless router located in close proximity. However, if the network connection is secure, a password is required to access the wireless network.

labeled "Jarvis," which the Portable Wireless Detector identified as password protected.[2] Agent Fiore did not seek to verify with the users of the wireless networks in the condominium complex whether the networks they were using were secure because he was concerned about maintaining the secrecy of his investigation.

On February 8, 2012, other law enforcement officers engaged in surveillance of the Residence and observed wireless networks in the area using a device in their vehicle. This device indicated that there were twenty-nine wireless networks, eight of which were unsecure.

Agent Fiore drafted the search warrant application and supporting Affidavit to search the Residence for electronic and other communications pertaining to child pornography. The Affidavit does not include information regarding the existence of secure or unsecure wireless networks. However, it states that it "does not contain every fact known to [Agent Fiore] with respect to this investigation. Rather it contains those facts that [Agent Fiore] believe[d] to be necessary to establish probable cause for issuance of a search warrant for the [Residence]." (Doc. 33-1 at 7-8) Agent Fiore testified that he did not believe it was necessary to include in the Affidavit information regarding the presence of unsecure wireless networks in the area surrounding the Residence or that the "Jarvis" network was secure in order to establish probable cause. He noted that the United States Attorney's office reviewed and approved the Affidavit for probable cause prior to its submission to the Magistrate Judge. On February 23, 2012, United States Magistrate Judge John Conroy issued a search warrant for the Residence.

Defendant challenges Agent Fiore's credibility, based upon what he claims was a falsehood in a separate report created by Agent Fiore, wherein Agent Fiore stated that he "observed a wagon parked next to the building [at 648D Old Hollow Rd., North Ferrisburgh, VT] [bearing] Vermont registration FLE546 . . . registered to Tor C. Borgstrom" and that "[a] public records check of Tor[.] C. Borgstrom show[ed] . . . a

[2] Agent Fiore is aware of instances where police have searched a house, based on activity from an IP address associated with the house, and have found no evidence because the wireless network in the house was unsecure.

current address of 648D Old Hollow Rd., North Ferrisburgh, VT." (Gov. Ex. 4 at 3-4.) Defendant called Mr. Borgstrom as a witness, and he testified that he no longer lived at the North Ferrisburgh address and at the time did not possess a vehicle that could accurately be described as a "wagon." The court finds any discrepancy in Agent Fiore's supplemental report regarding an unrelated vehicle identification immaterial and finds Agent Fiore's testimony credible.

II. Conclusions of Law and Analysis.

Defendant seeks suppression of the evidence discovered during the March 2, 2012 search of the Residence, arguing that Agent Fiore deliberately or with reckless disregard for the truth omitted from the Affidavit information regarding the existence of secure and unsecure wireless networks in the area surrounding the Residence. He argues that the omitted information was material because, had it been included in the Affidavit, Magistrate Judge Conroy would not have found probable cause to search the Residence. The Government contends that probable cause existed with or without the omitted information and there is no evidence of any deliberate or reckless omission.

The Fourth Amendment provides that "no warrants shall issue, but upon probable cause, supported by Oath or Affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. A magistrate judge must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). "This required nexus between the items sought and the 'particular place' to be searched protects against the issuance of general warrants[.]" *United States v. Clark*, 638 F.3d 89, 94 (2d Cir. 2011).

"A search warrant affidavit is presumed reliable." *United States v. Klump*, 536 F.3d 113, 119 (2d Cir. 2008). A defendant may nonetheless challenge a search warrant "where the affidavit in support of the search warrant is alleged to contain deliberately or recklessly false or misleading information." *United States v. Canfield*, 212 F.3d 713, 717 (2d Cir. 2000). A defendant must show "by a preponderance of the evidence, that there

were intentional and material misstatements or omissions[,]" *Klump*, 536 F.3d at 119, that affected the finding of probable cause. *See Franks v. Delaware*, 438 U.S. 154, 156 (1978) (explaining that defendant has the burden of showing "perjury or reckless disregard" and "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause[.]").

A. Whether the Omitted Information Was Material to the Probable Cause Determination.

In this case, Defendant challenges the Affidavit based upon omitted information regarding the existence of multiple unsecure wireless networks in proximity to the Residence.[3] Information omitted from an affidavit is material only if it affects a finding of probable cause. In other words, a warrant is invalid, "*only* if the affidavit as supplemented by the omitted material *could not* have supported the existence of probable cause." *United States v. Lueth*, 807 F.2d 719, 726 (8th Cir. 1986); *see also United States v. Garza*, 980 F.2d 546, 551 (9th Cir. 1992) (refusing to suppress evidence when, "[e]ven if the misstatements were corrected and the omissions supplied, the affidavit would furnish probable cause for issuance of the warrant.").

The Government argues that the omission of information regarding the presence of unsecure wireless networks from the Affidavit was immaterial for two reasons. First, it

---

[3] Defendant relies on *United States v. Vosburgh*, 602 F.3d 512 (3d. Cir. 2010), wherein the court noted that, "[i]n those cases where officers know or ought to know . . . that an IP address does not accurately represent the identity of a user or the source of a transmission, the value of that IP address for probable cause purposes may be greatly diminished, if not reduced to zero." *Id.* at 527 n.14. Defendant also points to cases that explain how unauthorized third parties may utilize an IP address associated with an unsecure wireless network and argues that, because of this possibility, Agent Fiore knew or should have known that the IP Address may not accurately represent the source of the transmission. *See United States v. Griswold*, 2011 WL 7473466, at *1 (W.D.N.Y. June 2, 2011) ("Concerned that the IP address under investigation could have been accessed by someone not associated with the residence, [officers] decided to knock on the door of the residence and try pursuing their investigation without a search warrant."); and *State v. Bailey*, 2010 ME 15, ¶ 5, 989 A.2d 716, 719 ("The officers did not discover either the target computer or any child pornography during the execution of the warrant; instead, they determined that the IP address sharing the files was associated with an unsecured wireless router located at that residence. In other words, someone within range of the router was using it to access a peer-to-peer network and disseminate the files in question.").

asserts that probable cause to search the Residence would have existed even if the IP Address was associated with an unsecure wireless network. As it points out, courts have consistently concluded that there is probable cause to search a residence when an IP address associated with child pornography can be traced to the residence. *See United States v. Haymond*, 672 F.3d 948, 958 (10th Cir. 2012) (finding that a supporting affidavit, which stated "that [the officer] observed a user with an IP address linked to [defendant's] residence who had numerous files of child pornography available[,]" was sufficient to establish probable cause); *United States v. Stults*, 575 F.3d 834, 843-44 (8th Cir. 2009) (concluding that the affidavit, which, among other things, "stated that an IP address traced to [defendant] was identified as accessing child pornography sites[,]" created probable cause to search defendant's residence); *United States v. Perez*, 484 F.3d 735, 740-42 (5th Cir. 2007) (finding probable cause that evidence would be found at the physical address associated with the IP address from which child pornography was transmitted). Here, the Affidavit clearly establishes that nexus.

Moreover, courts have generally concluded that the mere possibility that an IP address may be associated with an unsecure wireless network does not affect the probable cause determination.[4] Although the presence of unsecure wireless networks gives rise to the possibility that a person outside of the Residence may have accessed the network to

[4] *See Perez*, 484 F.3d at 740 (rejecting defendant's arguments that neighbors could have used his IP address if his network was unsecure, the court explained that "it was possible that the transmissions originated outside of the residence to which the IP address was assigned, [but] it remained likely that the source of the transmissions was inside that residence."); *United States v. Grant*, 218 F.3d 72, 75 (1st Cir. 2000) (acknowledging that a user other than an account registrant may have access to a registrant's account, the court nonetheless explained that "there is no evidence suggesting that on any given occasion, the user is not likely in fact to be the registrant. Thus, even discounting for the possibility that an individual other than [the registrant] may have been using [the registrant's] account, there was a *fair probability* that [the registrant] was the user and that evidence of the user's illegal activities would be found in [the registrant's] home."); *United States v. Chamberlin*, 2010 WL 1904500, at *7 (W.D.N.Y. May 12, 2010) (finding "unpersuasive [defendant's] argument that the search warrant application lacked probable cause because of the possibility that another person or computer could have gained access to the internet using [defendant's] IP address[,]" explaining that "it was reasonable to assume that the address associated with the IP address was responsible for activity connected to that IP address[.]").

transmit messages regarding child pornography, it remains probable that the transmission originated from within the Residence and that evidence of child pornography would be found there. *See Maryland v. Pringle*, 540 U.S. 366, 371 (2003) ("The probable-cause standard is incapable of precise definition or quantification into percentages because it deals with probabilities and depends on the totality of the circumstances."); *United States v. Martin*, 426 F.3d 83, 86 (2d Cir. 2005) ("[P]robable cause only requires 'the probability, and not a prima facie showing, of criminal activity.'") (quoting *Gates*, 426 U.S. at 235).

Second, the Government contends that inclusion of the omitted information in the Affidavit would have strengthened, not weakened, the argument for probable cause. Although Defendant argues that the known presence of unsecure wireless networks means that someone other than an occupant of the Residence could have used the IP Address, he does not contend that this could occur if the IP Address was associated with a secure wireless network. The information omitted from the Affidavit included evidence that the "Jarvis" wireless network was a secure wireless network. Accordingly, some of the information Defendant argues was deliberately or recklessly omitted from the Affidavit made it *more likely* that child pornography would be found at the Residence.

Because the omitted information would not have materially affected the probable cause determination and because probable cause existed even in its absence, Defendant's challenge to the validity of the search warrant for lack of probable cause must fail.

B. Whether the Information Was Omitted Deliberately or With Reckless Disregard for the Truth.

Having concluded that the omitted evidence was not material to the probable cause determination, the court need not consider whether it was omitted deliberately or with reckless disregard for the truth. The court nonetheless observes that there is no evidence before the court that Agent Fiore concealed any evidence from the magistrate judge. Indeed, as noted, a key part of the information omitted -- that the "Jarvis" wireless network was secure -- would have *strengthened* the nexus between the IP Address and the Residence, making it *more likely* that child pornography would be found in Ms.

Jarvis's home. The presence of other unsecure wireless networks in the area in no way alters this conclusion.

CONCLUSION

For the foregoing reasons, Defendant's Motion to Suppress (Doc. 28) is DENIED. SO ORDERED.

Dated at Rutland, in the District of Vermont, this 15th day of October, 2012.

Christina Reiss, Chief Judge
United States District Court